UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/760,592	01/20/2004	Scott N. Gerard	ROC920030316US1	1109

30206 7590 03/21/2007

IBM CORPORATION
ROCHESTER IP LAW DEPT. 917
3605 HIGHWAY 52 NORTH
ROCHESTER, MN 55901-7829

EXAMINER	
BAYOU, YONAS A	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/760,592	GERARD, SCOTT N.	
	Examiner	Art Unit	
	Yonas Bayou	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/20/2004 and 03/03/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-11, 13, 14, 17-27 and 29-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-11, 13, 14, 17-27 and 29-34 are directed initiating performance of a computation, partitioning the computation, generating at least one distractive computational unit and initiating execution of computation.

This claimed subject matter lacks a practical application of a judicial exception (law of nature, abstract idea, natural occurring phenomenon) since it fails to produce a useful, concrete and tangible result.

Specifically, the claimed subject matter doesn't produce tangible result because the claimed subject matter fails to produce a result that is limited to having real world value rather than a result that may be interpreted to be abstract in nature as, for example a computation. More specifically, the claimed subject matter provides a method of initiating distributed computation in untrusted computing environments. This produced result remains in the abstract and, thus, fails to achieve the required status of having real world value.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-4, 6-20 and 22-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Jakobsson et al. US Patent Number 6,950,937 (hereinafter Jakobsson).

Referring to claims 1, 17 and 33 Jakobsson teaches a method which inherently teach an apparatus and program code of initiating performance of a computation on at least one untrusted computer, the method comprising:
partitioning the computation into a plurality of computational units that are combinable to generate a result for the computation;
generating at least one distractive computational unit;
initiating execution of both the at least one distractive computational unit and at least one of the plurality of computational units on the untrusted computer to

inhibit reconstitution of the computation by an untrusted party **[column 2, lines 12-16; column 3, lines 15- 52; column 4, lines 20-48 and figs. 1-3;** instead of referring to partitioning the computation into a plurality of computational units, generating at least one distractive computational unit and initiating execution of both computations on the untrusted computer, Jakobsson teaches division of the process into task transformation (partitioning of computation) which contains replication, dependency, blinding and random computation, such that replication, dependency and random permutation operation corresponds to a plurality of computational units where as blinding operation corresponds to one distractive computational unit and also result transformation corresponds to initiating execution of computations].

Referring to claims 2 and 18, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein the distractive computational unit comprises a computational unit generated from partitioning a second computation **[column 2, lines 12-16; column 4, lines 20-55 and figs. 3-7].**

Referring to claims 3 and 19, Jakobsson teaches a method which inherently teach the program code as applied above. Furthermore, Jakobsson teaches a method, wherein initiating execution of both the at least one distractive computational unit and at least one of the plurality of computational units includes interleaving the at least one distractive computational unit among multiple

computational units from the plurality of computational units **[column 5, lines 17-58 and fig. 3].**

Referring to claims 4 and 20, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation uses a different algorithm than that used to partition the second computation **[column 4, lines 56-67].**

Referring to claims 6 and 22, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein the distractive computational unit comprises a computational unit generated from a second partitioning of the computation **[column 2, lines 12-16; column 5, lines 17-column 7, lines 51 and fig. 3].**

Referring to claims 7 and 23, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, further comprising initiating execution of at least one of the plurality of computational units on a second computer **[column 3, lines 30-45].**

Referring to claims 8 and 24, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, further comprising initiating execution of all of the plurality of computational units on the untrusted computer **[column 3, lines 30-45; column 3, lines 52-57 and fig. 1].**

Referring to claims 9 and 25, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation into the plurality of computational units comprises partitioning using the Chinese Remainder Theorem (CRT) **[column 4, lines 56-67** instead of referring to Chinese Remainder Theorem (CRT), Jakobsson teaches Digital Signature Algorithm].

Referring to claims 10 and 26, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein the computation includes a plurality of arguments, and wherein partitioning the computation into the plurality of computational units comprises: selecting a plurality of relatively prime moduli; and generating each computational unit by performing a modulo operation on each of the plurality of arguments using one of the plurality of relatively prime moduli **[column 1, lines 14-28 and column 5, lines 1-17].**

Referring to claims 11 and 27, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein selecting the plurality of relatively prime moduli includes selecting each modulus from a superset of relatively prime moduli, the method further comprising: partitioning a plurality of computations into multiple computational units using different sets of moduli selected from the superset of relatively prime moduli; and initiating execution of computational units from multiple computations on the untrusted computer **[column 5, lines 1- 17].**

Referring to claims 12 and 28, Jakobsson teaches a method which inherently teach the system claims as applied above. Furthermore, Jakobsson teaches a method, further comprising: receiving result data generated during execution of each of the plurality of computational units; and generating a result for the computation from the result data **[column 2, lines 5-24; column 4, lines 10-20 and fig. 1]**.

Referring to claims 13 and 29, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein the untrusted computer is coupled to a grid computing network **[column 3, lines 1-17 and fig. 1]**.

Referring to claims 14 and 30, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation is performed by a client computer coupled to the grid computing network **[column 3, lines 35-41]**.

Referring to claims 15 and 31, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation is performed by a broker computer coupled to the grid computing network, the method further comprising receiving the computation from a client computer **[column 4, lines 20-31; fig. 1 and fig. 3]**.

Referring to claims 16 and 32, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation, generating the distractive computational unit, and initiating execution of both the distractive computational unit and the one of the plurality of computational units on the untrusted computer are performed by at least one computer coupled to the untrusted computer, the method further comprising communicating the distractive computational unit and the one of the plurality of computational units to the untrusted computer **[column 2, lines 1-16; column 5, lines 17-colunm 7, line 51; fig. 1 and fig. 3].**

Referring to claim 34, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein the signal bearing medium includes at a recordable medium and a transmission medium **[column 30-52 and fig. 1].**

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which

said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 5 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jakobsson et al. US Patent Number 6,950,937 in view of Elbe et al. WO 02/48857 A2.

Referring claims 5 and 21, Jakobsson teaches a method of initiating performance of a computation on at least one untrusted computer [see claim 1 above]. Jakobsson further teaches a method wherein the distractive computational unit comprises a computational unit generated from partitioning a second computation **[column 4, lines 20-55 and figs. 3-7].** Jakobsson does not explicitly teach a method, wherein the distractive computational unit comprises a dummy computational unit. However, Elbe teaches that one type of cryto coprocessors performs "dummy" computation for the purpose of making harder

for an attacker to find out parameters of the "useful" crypto coprocessor algorithm **[page 3, paragraph 0023; page 4, paragraph 0047 and 0049].** Jakobsson and Elbe are analogous art because both teach useful computational algorithms.

Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to modify the method of Jakobsson to incorporate the "dummy" computation of Elbe because the processor type performing dummy computations is selected advantageously in random manner, so that an attacker, will never know which processor type carries out useful computations.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Yonas Bayou

March 5, 2007

JOSEPH DEL SOLE
SUPERVISORY PATENT EXAMINER
3/6/07